@H2020Secondo

@H2020Secondo

SECONDO Project

Secondo Project

For more information, please visit our site: secondo-h2020.eu

SCAN ME

CONSORTIUM

1 UNIVERSITY OF PIRAEUS

1 UBITECH ubiquitous solutions

1 FOGUS INNOVATIONS & SERVICES

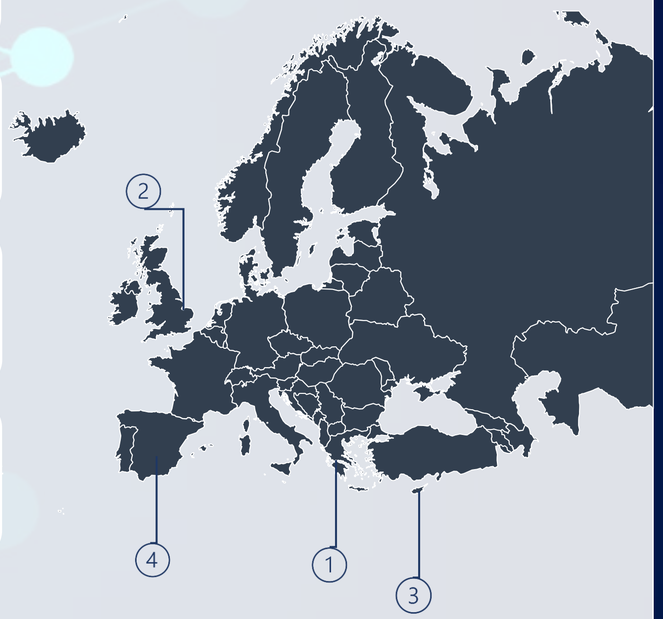
1 CROMAR INSURANCE BROKERS LTD

2 UNIVERSITY OF SURREY

2 UNIVERSITY of GREENWICH

3 Cyprus University of Technology

4 LS TECH Insightful Analytics



PROJECT COORDINATION

Prof. Christos Xenakis: School of Information and Communication Technologies Department of Digital Systems University of Piraeus Karaoli and Dimitriou 80,PC 18534, Piraeus, Greece

Tel: +30 210 4142776
email: xenakis@unipi.gr

This project has received funding from the European Union's H2020-MSCA-RISE-2018 program under grant agreement No 823997.

SECONDO

"A Security ECONomics service platform for smart security investments and cyber insurance pricing in the beyonD 2020 netwOrking era"

PROJECT DETAILS

Project number: 823997
Project Website: secondo-h2020.eu
Project start: 1st January 2019
Duration: 48 Months
Total cost: EUR 1 600 800
EC Contribution: EUR 1 600 800

Cyber Security Investment

The SECONDO project via its dedicated cybersecurity tool tailored for SMEs addresses the unique challenges faced by these businesses with limited budgets and resources. This tool serves as a strategic ally by conducting in-depth risk assessments specific to the SME's industry, operational model, and size. By identifying and quantifying potential risks, the tool assists SMEs in prioritizing cybersecurity investments where they will have the most significant impact. It goes beyond risk assessment to recommend cost-effective security solutions that align with the organization's risk tolerance and compliance obligations. One crucial aspect is the tool's role in fostering cybersecurity awareness and education among employees. SMEs often lack dedicated cybersecurity staff, making it essential for all employees to be vigilant. The tool can provide training modules and resources, empowering staff to recognize and mitigate potential threats. Moreover, the tool addresses the challenge of vetting third-party vendors by offering vendor assessment capabilities. This ensures that SMEs are not introducing additional risks through their supply chain, and it helps in maintaining a secure business ecosystem. Incident response planning is another critical feature of the tool, guiding SMEs in developing strategies to minimize the impact of cyber incidents. This proactive approach is particularly valuable in a landscape where cyber threats are continually evolving. Scalability is inherent in the tool's design, allowing SMEs to adjust their cybersecurity measures as they grow or as the threat landscape changes. This ensures that the organization's security posture remains robust and aligned with its expanding needs. A proactive monitoring approach allows SMEs to detect and respond swiftly to emerging cybersecurity issues, reducing the risk of successful attacks and minimizing potential damages. In summary, the tool not only optimizes resource allocation and guides strategic decision-making in cybersecurity investments but also acts as a comprehensive solution for education, incident response, vendor assessments, and scalable security measures. By addressing these aspects, the tool empowers SMEs to strengthen their cybersecurity defenses and navigate the intricacies of the digital landscape effectively, even within the constraints of a limited budget.

Building the human firewall

The Social Engineering Assessment Module is a crucial cybersecurity tool of the SECONDO platform designed to fortify an organization's defenses by concentrating on the establishment of a robust human firewall. This module goes beyond traditional technical assessments and recognizes the pivotal role that employees play in the cybersecurity landscape. It involves simulated social engineering scenarios, such as phishing emails to evaluate how well employees can withstand manipulation and recognize potential threats. The primary goal is not only to identify vulnerabilities but also to actively engage in the development of employee awareness and resilience. This is achieved through targeted training programs that educate staff about various social engineering tactics, the red flags associated with such attacks, and best practices for safeguarding sensitive information. By immersing employees in realistic scenarios and providing them with the knowledge and tools to respond effectively, the module contributes to the creation of a human firewall—a proactive defense mechanism against social engineering threats. Building a human firewall involves instilling a cybersecurity-conscious culture within the organization, where employees become the first line of defense against evolving social engineering tactics. The continuous assessment and educational components of the module ensure that the human firewall remains dynamic and adaptive in the face of emerging threats. Ultimately, by investing in the resilience of its workforce, an organization can significantly reduce the risk of successful social engineering attacks, creating a more robust and comprehensive cybersecurity posture.

Importance of a continuous cybersecurity risk monitoring tool

A continuous cybersecurity risk monitoring tool is a linchpin in the contemporary cybersecurity strategy, offering organizations an adaptive and vigilant shield against evolving threats. Unlike intermittent evaluations, continuous monitoring provides an uninterrupted stream of real-time insights into the intricate and ever-changing cybersecurity landscape. This immediacy enables swift detection of emerging threats, allowing organizations to respond proactively and mitigate risks promptly, thereby minimizing potential damages resulting from security incidents. The tool's dynamic nature is particularly crucial in an environment where cyber threats constantly evolve, providing organizations with the flexibility to adjust their security posture promptly in response to emerging vulnerabilities and attack vectors. By furnishing timely visibility into network activities, user behavior, and potential anomalies, the continuous monitoring tool empowers organizations to elevate their situational awareness, facilitating the early detection and mitigation of cyber threats. In essence, this not only contributes to a more resilient cybersecurity posture but also enables organizations to stay ahead of potential risks, reinforcing their ability to safeguard digital assets in an era of persistent and sophisticated cyber threats.

Cyber insurance premium calculation formula

The development of a cyber insurance premium calculation formula that takes into account a broad spectrum of parameters related to the contemporary cybersecurity landscape is crucial in responding to the dynamic and evolving nature of cyber threats. A comprehensive formula should consider the organization's overall cybersecurity posture, which includes factors such as the deployment of advanced security technologies, the frequency and effectiveness of security audits, and the sophistication of protective measures in place. Assessing incident response capabilities, employee training programs, and the organization's adaptability to emerging threats are equally critical aspects to include in the premium calculation. Moreover, the formula should factor in industry-specific risks, regulatory compliance adherence, and the organization's geographic exposure to cyber threats. The prevailing threat landscape, encompassing emerging cyber attack vectors and prevalent tactics, techniques, and procedures (TTPs) should also be incorporated into the premium calculation to ensure relevance and accuracy. This comprehensive approach not only tailors insurance coverage to the specific risk profile of each organization but also serves as a valuable tool in promoting proactive cybersecurity practices. By incentivizing the adoption of robust security measures, continuous improvement, and adherence to best practices, the premium calculation formula becomes a strategic mechanism for cultivating a cyber-resilient environment. Insured entities, motivated by the prospect of favorable premiums, are encouraged to invest in strengthening their cybersecurity defenses, resulting in a win-win scenario for both organizations and insurance providers. Ultimately, a well-crafted premium calculation formula aligned with the diverse facets of the cybersecurity landscape contributes to the creation of a more secure digital ecosystem.

Most common parameters that influence the premium:

- Base Rate
- Down Time
- Limit of liability
- Deductible
- Territory
- Claims-made
- Externed Reporting
- Credit
- Group
- Data Used
- Compliance

High-quality data in risk management lifecycle

Utilizing high-quality data is paramount in the realm of cybersecurity, particularly when conducting risk assessment. The significance of delving into the dark web and actively monitoring social media platforms for pertinent cybersecurity data cannot be overstated. The dark web, with its clandestine nature, serves as a breeding ground for cyber threats, housing forums, marketplaces, and communication channels where malicious actors discuss and exchange cyber tools, exploits, and sensitive information. Crawler tools navigating the dark web enable organizations to uncover potential threats, vulnerabilities, and indicators of compromise that may not be visible on the surface web. Simultaneously, monitoring social media platforms is crucial for tracking emerging trends, potential attacks, and discussions related to cybersecurity incidents. Threat actors often leverage social media for reconnaissance and communication, making it a valuable source for early threat detection. The amalgamation of dark web and social media data enriches the quality of information available for risk assessments, allowing organizations to proactively identify and mitigate cyber risks, fortify their defenses, and stay one step ahead of evolving threats in the digital landscape.

The impact of data quality in the realm of cyber insurance is pivotal, influencing every stage of the insurance process. High-quality data is the bedrock of accurate risk assessment, underwriting precision, and effective claims management. During risk assessment, reliable data enables insurers to evaluate a policyholder's cybersecurity posture accurately, ensuring informed decision-making and avoiding potential mispricing of policies. In policy underwriting, the use of accurate and comprehensive data is essential for setting coverage limits, determining exclusions, and establishing appropriate pricing. In the event of a cyber incident, quality data is crucial for swift and fair claims management, facilitating efficient claims processing and accurate quantification of financial impacts. Furthermore, high-quality data drives the continuous improvement of cyber insurance products, enabling insurers to refine underwriting models, enhance risk mitigation strategies, and stay ahead of emerging threats. Overall, the integrity of data directly shapes the effectiveness of cyber insurance, ensuring that coverage aligns with actual risk profiles, promotes resilience, and contributes to the ongoing development of the cybersecurity insurance industry.